Empresa de Generación Eléctrica San Gabán S.A.

# INFORME TÉCNICO DE SOFTWARE

San Gabán

## Software de Firma Digital

# INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE

## Nº 001-2018-DTI/GG

1. **NOMBRE DEL ÁREA:** División de Tecnologías de Información
2. **RESPONSABLES DE LA EVALUACIÓN:** Ing. César Castro Guzmán
3. **CARGOS:** Jefe de Tecnología de Información
4. **FECHA:** Noviembre 2018
5. **JUSTIFICACIÓN**

La Presidencia del Consejo de Ministros (PCM), a través de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) está impulsando la Firma Digital en el Gobierno Electrónico, por lo que está difundiendo entre los representantes de la Administración Pública la importancia de la Ley Nº 27269, Ley de Firmas y Certificados y su reglamento, así como las normas técnicas vinculadas a la materia.

San Gabán S.A. en concordancia con la Ley N° 27269 necesita integrar a su Sistema de Tramite Documentario el componente de firma digital, el mismo que contribuirá a la reducción del uso de papel, suministros y servicios relacionados a esta actividad en toda la organización. Por lo tanto, requiere adquirir un software de firma digital que brinde las facilidades de integración al Sistema de Trámite Documentario, el mismo que deberá estar acreditado ante la Autoridad Administrativa competente (INDECOPI) con el objetivo de asegurar que la solución cumple con todos los requisitos e interactúa directamente con la Infraestructura Oficial de Firma Electrónica (IOFE) del estado peruano, garantizando que los documentos firmados digitalmente a través de dicho software tengan el mismo efecto legal que una firma manuscrita en un documento físico.

6. **ALTERNATIVAS**

Para esta evaluación se han considerado los siguientes proveedores que cumplen con la acreditación otorgada por la Autoridad Administrativa Competente (INDECOPI).

- PeruSecure.NET
- Soft&Net Solutions

## 7. ANÁLISIS COMPARATIVO TÉCNICO

| Item | Especificaciones Técnicas | Puntaje | Puntaje Total | Puntaje Total |
|---|---|---|---|---|
| 1 | El software debe estar acreditado por INDECOPI por ser la Autoridad Administrativa Competente de la Infraestructura Oficial de Firma Electrónica (IOFE) de la República del Perú. | 5 | 5 | 5 |
| 2 | Debe permitir firmar digitalmente un documento y/o archivo electrónico a la vez. | 4 | 4 | 4 |
| 3 | Debe permitir efectuar múltiples firmas digitales en un mismo documento y/o archivo electrónico. | 4 | 4 | 4 |
| 4 | Debe permitir firmar digitalmente un lote de documentos y/o archivos electrónicos. | 4 | 4 | 4 |
| 5 | Debe permitir que la firma digital se incruste en el documento electrónico de modo que la firma puede ser visualizada junto con el documento. La posición de la firma debe ser configurable. | 4 | 4 | 4 |
| 6 | Debe permitir firmar documentos y archivos electrónicos en los formatos: PDF, DOC, XLS, GIF, JPG, TIFF, MP3, MP4 y XML, debiendo usarse los estándares de firma CAdES, XAdES y PAdEs. | 5 | 5 | 5 |
| 7 | Debe permitir la incrustación de sello de tiempo (RFC-3161) al momento de realizar la firma digital en cualquier documento y/o archivo electrónico. | 4 | 4 | 4 |
| 8 | Debe permitir visualizar la información referida a la ruta de certificación de todas las firmas digitales del documento | 4 | 4 | 4 |
| 9 | Debe permitir visualizar la información de la firma y el certificado asociado | 3 | 3 | 3 |
| 10 | Debe permitir pre-visualizar el documento para ubicar la posición, el tamaño y una imagen personalizada opcional para crear una firma visible en el documento para identificar visualmente las firmas antes de firmar el documento digitalmente. | 3 | 3 | 3 |
| 11 | Debe permitir que el documento electrónico y/o archivo sea visualizado antes del proceso de firma | 3 | 3 | 3 |
| 12 | Debe permitir verificar el estado de revocación de un certificado digital. | 3 | 3 | 3 |

| | | | | |
|---|---|---|---|---|
| 13 | Debe permitir verificar<br>- La firma digital en un documento y/o archivo electrónico.<br>- Las firmas digitales múltiples en un solo documento y/o archivo electrónico.<br>- Las firmas digitales en un lote de documentos y/o archivos electrónicos.<br>Esta verificación consta de lo siguiente:<br>• Constatar la integridad del documento firmado. La integridad se refiere a que el documento y/o archivo electrónico no ha sido alterado desde que fue firmado.<br>• Constatar la autenticidad del documento y/o archivo electrónico firmado.<br>• Validar que al momento de la firma el certificado digital se encuentre vigente.<br>• Permitir obtener la TSL (Trusted Services List) oficial del INDECOPI ("Lista de Proveedores de Servicios Confiables" o "Trusted Services List"), para la verificación de la ruta de certificación del certificado. | 5 | 5 | 5 |
| 14 | Debe permitir verificar su consistencia y verificar si el certificado raíz del firmante se encuentra autorizado dentro de la IOFE (Infraestructura Oficial de Firma Electrónica de la República del Perú). | 3 | 3 | 3 |
| 15 | Debe permitir verificar la revocación utilizando el protocolo OCSP (Online Certificate Status Protocol), en caso no esté disponible se debe proceder a verificar la revocación por el protocolo CRL (Certificate Revocation List), en caso la CRL no esté disponible la aplicación no debe permitir que se aplique la firma digital. | 3 | 3 | 3 |
| 16 | Debe disponer de un módulo de validación que permita verificar la integridad del documento firmado digitalmente de los diferentes formatos. De ser posible, gestionar los errores de firma digital, almacenando la información en base de datos. | 3 | 3 | 3 |
| 17 | El software de firma digital debe estar basado en tecnología WEB. | 3 | 3 | 3 |
| 18 | El software de firma digital debe ser compatible mínimo con los siguientes navegadores Web: Internet Explorer, Mozilla Firefox y Google Chrome | 3 | 3 | 3 |
| 19 | Debe permitir la Integración con los diferentes lenguajes de programación como Java, C#, .NET, Python, Abap, PowerBuilder, etc. | 3 | 3 | 3 |
| 20 | El software de firma digital debe soportar todos los dispositivos criptográficos que cumplen con los siguientes estándares:<br>• Certificaciones: FIPS 140-2 Level 1 o superior, o Common Criteria EAL4 o superior.<br>• Longitud de claves: RSA de 2048 bits. - Algoritmos de hash · SHA-1, y SHA-2, SHA – 256, SHA 512.<br>• Algoritmos de firma · RSA with SHA1, RSA with SHA2 y RSA with SHA256.<br>• Almacenamiento de certificados X.509 v3. El software de firma digital debe soportar certificados digitales según este formato X.509 v3.<br>• Estándares:<br>o ISO 7816: 1, 2, 3, 4, 8, 9 (Smart Card de contacto de tamaño ID-1).<br>o Protocolo CCID. Protocolo que permite conectar una tarjeta inteligente a una computadora a través de un lector de tarjetas | 5 | 5 | 5 |

| | | | | |
|---|---|---|---|---|
| | utilizando una interfaz USB estándar.3 | | | |
| 21 | El software debe ser compatible con los sist3emas operativos: Microsoft Windows XP, 7, 8.1, 10 (32 bits y 64 Bits), Ubuntu, CentOS, Red Hat, Fedora. | 3 | 3 | 3 |
| 22 | API criptográfico compatible:<br>- PKCS#11: Dependencias (Dynamic-Link Library .dll) que implementan el estándar PKCS#11 para Windows 7 (64 bits) y Red Hat.<br>- Microsoft CryptoAPI (CSP). | 3 | 3 | 3 |
| 23 | El software de firma digital debe soportar aquellos certificados digitales emitidos por entidades certificadoras que trabajen con el estándar X.509. | 3 | 3 | 3 |
| 24 | El software de firma digital debe contar con un componente de integración web que soporte los lenguajes de programación web más comerciales: JAVA, Visual Basic 6, .Net, PHP y multiplataforma (en servidores Windows, Linux, Unix). Este componente de integración web debe ser configurable a través de parámetros de entrada y que se pueda comunicar con el lado servidor a fin de garantizar la seguridad de las peticiones de firma digital, por tanto, el Software de Firma Digital a través de este componente se debe integrar con las aplicaciones en cualquier proceso y/o sistema. | 3 | 3 | 3 |
| 25 | El software de firma digital debe tener la capacidad de firmar masivamente documentos electrónicos en el servidor o aplicaciones cliente, tomando como entrada la ruta de origen de los documentos a firmar, la ruta destino, referencia del certificado digital a utilizar (de suscriptor o agente automatizado), servicio de sello de tiempo y otros parámetros requeridos para la firma de conformidad con la guía de acreditación de software para firmas digitales. | 3 | 3 | 3 |
| 26 | La solución de firma digital permite realizar firmas con certificados digitales almacenados desde un dispositivo criptográfico tipo token, tarjeta inteligente (Smart card), DNI-E o módulo de seguridad de Hardware (hardware security module – HSM) | 3 | 3 | 3 |
| 27 | Debe permitir obtener o visualizar la trazabilidad del proceso de firma digital en su aplicativo. | 5 | 5 | 5 |
| 28 | El software integrado a la aplicación web solicitará el Certificado Digital. Este podrá encontrarse instalado en el equipo, token, smartcard o DNIe. | 3 | 3 | 3 |
| 29 | El software solicitara el pin del certificado. | 3 | 3 | 3 |
| | **TOTAL** | **100** | **100** | **100** |

## Licencia – Costo

| Nombre proveedor | Características | Importe en S/ incluido IGV |
|---|---|---|
| **Peru Secure Net S.A.C.** | **Licencias de Software** | |
| | a) Componente de Servidor, licencia perpetua | 61,250.00 |
| | b) Componente de Clientes, licencias perpetuas | 47,730.00 |
| | Servicio de integración del software de firma digital con el software de SEGDI incluido en el costo | |
| | **TOTAL** | ***108,980.00*** |
| **Soft & Net S.A.C.** | Software de firma digital centralizada versión web, incluye:<br><br>- **Licencia anual**<br>- Servicio de integración con una aplicación<br>- Soporte y mantenimiento durante el primer año<br>Garantía de 01 año. | 32,000.00 |
| | **TOTAL** | **31,000.00** |

## Evaluación comparativa técnica

De acuerdo a la evaluación técnica y teniendo en consideración los aspectos necesarios que se requiere se tiene los siguientes resultados.

| Software | Puntaje |
|---|---|
| Peru Secure Net S.A.C. | 100 |
| Soft & Net S.A.C. | 100 |

## 8. ANÁLISIS COMPARATIVO DE COSTO – BENEFICIO

| Concepto | Peru Secure Net S.A.C. | Soft & Net S.A.C. | Observaciones |
|---|---|---|---|
| Licenciamiento | S/ 108,980.00 | S/ 31,000.00 | Licencias perpetuas |
| Hardware necesario para | No | No | Usa la infraestructura |

| | | | |
|---|---|---|---|
| su funcionamiento | | | existente |
| Soporte y mantenimiento externo | Si | Si | Actualizaciones automáticas |
| Personal y mantenimiento interno | Si | Si | Opcional Manuales técnicos disponibles |
| Capacitación | Si | Si | |
| COSTOS TOTALES | S/ 108,980.00 | S/ 31,000.00 | |

Los precios no incluyen IGV

| Análisis Cualitativo | Selección Evaluación Técnica | Selección Evaluación Económica |
|---|---|---|
| **BENEFICIO / COSTO** | Soft & Net S.A.C. | Soft & Net S.A.C. |

## 9. CONCLUSIONES

Se determinó los atributos o características técnicas mínimas que deben ser considerados para una evaluación de software, asimismo se estableció la valoración cuantitativa de cada característica y los costos de licenciamiento en cada caso. Por lo anteriormente expuesto consideramos que el software que mejor se adecua a nuestras necesidades es el proporcionado por el proveedor Soft & Net S.A.C.

## 10. FIRMAS

ING. CESAR CASTRO GUZMÁN-MBA
JEFE DE TECNOLOGÍA DE LA INFORMACIÓN
SAN GABÁN S.A.